Государственное бюджетное общеобразовательное учреждение

г. Санкт-Петербург «Средняя школа №458»

Итоговый индивидуальный проект на тему

«Кодирование и шифрование»

Выполнил: Выдра Андрей Михайлович 10-2 класс

Руководитель: Сизов Вадим Евгеньевич (ГБОУ СОШ №458)

**Оглавление**

1. Введение в проект3  
   1.1. Введение3
2. Введение в теорию кодирования и шифрования4
   1. Кодирование и шифрование5-6
   2. Азбука Морзе6-8
3. Создание приложения по декодированию/кодированию шифрованию8
   1. Идея приложения8
   2. Техническое задание9
   3. Создание дизайна приложения10
   4. Написание кода10
   5. Тестирование и отладка10-11
4. Заключение12  
   4.1. Заключение12  
   4.2. Будущее проекта12
5. Список используемой литературы13

**ГЛАВА I. ВВЕДЕНИЕ В ПРОЕКТ**

* 1. **Введение**

Жизнь современного человека не обходится без современных технологий. Мы активно пользуемся вещами в нашей жизни, которые были созданы благодаря достижениям научно-технического прогресса, но даже не представляем, как они устроены. Умные дома, смартфоны, квантовые компьютеры – все эти вещи берут своё начало, ещё задолго до появление первого калькулятора. Истоки этих передовых технологий напрямую связаны с кодированием и шифрованием. Данные термины ассоциируются у человека с чем-то инновационными, хотя первые упоминания этих понятий появляются с глубокой древности. К примеру, шифрование начинает использовать Гай Юлий Цезарь для переписки со своими генералами. Шифр, который он придумал, назван «Шифр Цезаря» и в своё время пользовался популярностью ещё долгое время. Между двумя понятиями (кодирование и шифрование) найти разницу достаточно сложно, в современной речи данные слова имеют схожие значения, хотя несут совершенно противоположные смыслы.

Современные технологии постоянно используют различного рода кодировки для достижения большей эффективности с уменьшением затрат, а в свою очередь шифрование применяется для сокрытия какой-либо информации от посторонних лиц. Методы шифрования и кодирования постоянно усложняются, развиваются и модернизируются, поэтому тема проекта совершенно актуально и в наше время.

Цель работы: Изучение принципов работы кодирования и шифрования

Задачи работы:

1. Изучить историю кодирования и шифрования
2. Выяснить как устроено кодирование и шифрование
3. Создать приложение по кодированию (шифрованию) и декодированию (дешифрованию) какого-либо текста, используя Азбуку Морзе

Результат проекта (продукт): электронная презентация, приложение.

Основная задача приложения – познакомить пользователя с основами кодированием (шифрованием) и декодированием (дешифрованием). Продукт и исследование данного проекта может использоваться в образовательных целях.

**ГЛАВА II. ВВЕДЕНИЕ В ТЕОРИЮ КОДИРОВАНИЯ И ШИФРОВАНИЕ  
2.1. Кодирование и шифрование**

Как и говорилось ранее, кодирование и шифрование информации близкие по смыслу термины, но означают они всё же разные вещи:

*Кодирование информации* - процесс преобразования сигнала из формы, удобной для непосредственного использования информации, в форму, удобную для передачи, хранения или автоматической переработки. С помощью кодированию мы можем мы можем обмениваться данными между собой и работать с ними так, как удобно это нам. В качестве примера можно привести русский алфавит, благодаря которому мы передаём мысли при помощи звуков, которые понимают все люди, знающие русский язык, т.е. определённую кодировку. Примеры кодирования:

* Нотная грамота — кодирует музыку;
* Дорожные знаки и сигналы светофора кодируют правила дорожного движения;
* Иконки в смартфоне — кодируют информацию о приложении;

*Шифрование данных*- это методы защиты любой информации от несанкционированного доступа, просмотра, а также её использования, основанные на преобразовании данных в зашифрованный формат. Такие данные могут прочитать только те, кто обладает особым знанием (ключ, сертификат и т.п.). Цель шифрования обратна цели кодирования – скрывать данные от всех, у кого нет ключа расшифровки. Примеры шифрования:

* Банки защищают хранить информацию об их клиентах;
* Мессенджеры защищают переписку от злоумышленников;
* Цифровая валюта;
* Сайты шифруют пароли пользователей, чтобы никто не мог их узнать;

Существует различное множество различных шифров. Одними из самых популярных и простых для понимания являются:

* Шифр Цезаря (основан на сдвиге алфавита на какое-то количество знаков). Например, сообщение «выпей чаю» может стать «еютзм ъгб», если сдвиг алфавита будет равен трём.
* Азбука Морзе (основан на замене букв и символов на точки и тире). К примеру, слово «Да» можно зашифровать, как «−•• •−».

Данные шифры уже давно не используются в технологиях и военной сфере, потому что они утратили свою засекреченность и ключ для расшифровки может получить обычный человек. Можно сказать, что эти коды являются чем-то между кодировкой и шифром из-за своей популярности и доступности. Об одном из них дальше и пойдёт речь.

**2.2. Азбука Морзе**

Азбука Морзе - способ знакового кодирования, представление букв алфавита, цифр, знаков препинания и других символов последовательностью сигналов: длинных (тире) и коротких (точек).

История создания:

Натолкнуло Морзе на мысль создать быстрый способ передачи информации печальное событие. В 1825 году Сэмюэл получил письмо от отца, где говорилось, что его жена находится при смерти. Конечно, Морзе сразу отправился в путь, но не успел. К его приезду его любимая жена скончалась. Это событие так потрясло Морзе, что он решил создать такую систему, с помощью которой можно было передавать сообщения на дальние расстояния. Однако на это ушло больше десяти лет. Уже в 1844 году был послан первый сигнал длиной 1700 футов, текст которого был таким: «Чудны дела твои, Господи!».

Принципы работы Азбуки Морзе:

* Код Морзе является двоичным, т.е. код состоит только из 2 символов, а именно точек и тире.
* Количество допустимых символов (букв, цифр, знаков препинания и т.п.) для кодировки определяется как 2n, где n – количество точек и тире.

**Количество кодов = 2количества точек и тире**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Кол-во точек и тире | 1 | 2 | 3 | 4 |
| Количество получаемых кодов | 2 | 4 | 8 | 16 |

* Отсутствие условия Фано.  
  Условие Фано - *Никакое кодовое слово не может быть началом другого кодового слова*В Азбуке Морзе буква А кодируется ⋅, но при этом будет существовать символ Б, код которого будет представлять ⋅-.
* Существование таблицы перевода  
  *Буква алфавита* → *последовательность азбуки Морзе, состоящая из точек и тире*.

Но отсутствие таблицы. *Алфавит из точки и тире* → *буква человеческого алфавита.*

Недостатки:

* Неэкономичность, на передачу одного знака кода требуется в среднем 9.5 элементарных посылок;
* Малая пригодность для буквопечатающего приёма (из-за переменной длины кода);
* Низкая скорость телеграфирования (из-за переменной длины кода необходимость длинных пауз между передаваемыми символами).

Достоинства

* Высокая помехозащищённость при приёме на слух в условиях сильных радиопомех;
* Возможность кодирования вручную;
* Узкая полоса занимаемых частот;
* Запись и воспроизведение сигналов простейшими устройствами.

Азбука Морзе является примером бинарного кода, современные компьютеры работают по принципу работы двоичных кодов, т.к. простейшими сигналами работы компьютера являются отсутствие тока и его присутствие, а также все данные, находящиеся на вашем компьютере, на низшем уровне кодируются нулями и единицами. Простейшие шифры заложили фундамент для создания безотказных вычислительных машин.

**ГЛАВА III. Создание приложения по кодированию и декодированию информации.  
3.1. Идея приложения**

Задумкой приложения является познакомить пользователя с шифрованием и кодированием. За основу работы программы будет взята Азбука Морзе. Выбор был сделан в пользу данного шифра из-за его относительной простоты и наглядного применения. Цикл создания приложения можно разбить на несколько основных логических частей:

1. Создание технического задания с объяснением того, как приложение будет выглядеть, а также, как именно пользователь должен взаимодействовать с программой.
2. Создание дизайна для приложения
3. Написание программного кода
4. Тестирование и отладка приложения

**3.2.** **Техническое задание**

*Техническое задание* – документ, который определяет цель, функционал и структуру приложения.

Программа будет представлять из себя оконное приложение, в котором можно будет выбрать режим работы (кодирование/декодирование). В приложении будет доступно поле ввода информации, поле вывода ответа и кнопка, по нажатию на которую будет происходить кодирование/декодирование, в зависимости от выбранного вами режима.

Приложение будет написано на языке программирования Python и использовать дополнительную библиотеку PyQt5

**3.3. Создание дизайна приложения**

Как говорилось ранее, приложении будет представлять из себя оконный формат, поэтому немалая часть работы будет связана с созданием дизайна моего приложения. При создании внешнего облика программы важно учитывать следующие факторы:

* Доступность для широкого пользователя
* Простота в использовании

Для создания внешнего вида, я буду использовать QT designer – приложение по созданию дизайнов для программ. Основные цвета дизайна следующие: серые, тёмные. Данная гамма была выбрана, потому что в актуальных программах всё больше набирают популярность тёмные цвета из-за того, что от них человеческие глаза меньше устают, чем от светлых тонов. Внешний вид программы относительно прост: всего два окна (ввод текста и ввод символов Азбуки Морзе) и кнопка кодировать, сверху также присутствует панель навигации, где можно сменить режим кодировать/декодировать.

**3.4. Написание кода**

Программа написана на языке Python (версия 3.9) с использованием библиотеки PyQT. Для создания кода использована интегрированная рабочая среда PyCharm. При создании программы задействован объектно-ориентированный подход. Код делиться на абстрактные сущности, функции и методы, а также соответствует рекомендациям и практикам, применяемыми инженерами. Приложение собрано в файл с расширением .exe, для

**3.4. Тестирование и отладка**

Важной частью создания приложения является его «Проверка на надёжность». Нередко случается так, что в созданной программе присутствуют ошибки, которые нужно исправить. Данный процесс можно поделить на несколько видов:

* Отладка – поиск и устранение синтаксических ошибок в написании кода
* Тестирование – проверка программы на работоспособность.

Так, например, я столкнулся с несколькими этими обоими видами ошибок. Если провести отладку достаточно просто из-за того, что большее количество данного вида ошибок происходит из-за опечаток, то полноценное тестирование часто затрачивает большее количество времени.

На следующем примере, с которым я столкнулся, будет показан принцип тестирования:

1. Запуск программы
2. Имитация действий пользователя для проверки функциональности
3. Обнаружение ошибки: текст, зашифрованный в Азбуку Морзе, был переведён некорректно
4. Обдумывание конкретной проблемы: ошибка вызвана некорректным вводом или неправильным алгоритмом переводом?
5. Нахождение решения: ошибка вызвана некорректным вводом пользователя (пользователь не отделял буквы, переведённые в Азбуку Морзе, пробелами), который не был ограничен программно.
6. Исправление ошибки: выведение предупреждения о том, что текст буквы должны вводится через пробел.

**ГЛАВА IV. ЗАКЛЮЧЕНИЕ**

**4.1. Заключение**

Представленный проект был посвящён теме «Кодирование и шифрование». В процессе выполненной работы я узнал много чего нового, как создать своё приложение, о том, что из себя представляет теория кодирования и шифрования. Были изучены многие источники, как свободные интернет ресурсы, так и научная литература. Данный проект может помочь в изучении представленной теме и другим людям: подросткам и взрослым. На создание проекта ушло большое количество сил и времени, и я считаю, что данный продукт является качественным и может помочь людям совершенствовать их навыки.

**4.2. Будущее проекта**

Данный проект был опубликован на сервисе Github (международный сервис обмена IT проектов) и доступен для любого человека. Ссылка на него – [https://github.com/andreyvydra/morz](https://github.com/andreyvydra/morz%20). В будущем планируется реализовать улучшенный функционал – добавление справочной информации в приложение, звуков для азбуки Морзе и другое.

**ГЛАВА V. СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ**

1. Кодирование и шифрование - в чём разница? // Журнал Код URL: <https://thecode.media/symbols/>
2. Чарльз Петцольд / Код. Тайный язык информатики. - 2-е изд. - Москва: Манн, Иванов и Фербер, 2020. - 448 с.
3. Роберт Мартин / Чистый код. Создание, анализ и рефакторинг. -1-е изд. – Санкт-Петербург: Питер, 2021. – 464 с.
4. Кодирование и Шифрование // Хабр URL: <https://habr.com/ru/post/548304/>
5. Иванов Г. Г., Красносельский Б. М. Радиооператор. — М.: ДОСААФ, 1976
6. Красовский М. М. Азбука Морзе. Приём на слух и работа на ключе // Дешёвая библиотека журнала «Радио всем», вып. 19. — М.: Государственное издательство, 1927
7. Гай Светоний Транквилл. Жизнь двенадцати цезарей = De vita XII caesarvm. — М.: Издательство «Наука», 1964. — 374 с.
8. МАТЕМАТИКА. Полная энциклопедия / Акулич, Башмакова, Васильев и др. – М.: РОСМЭН, 2020, - 256 с.: ил.
9. Документация для PyQt5 // QT documentation: <https://doc.qt.io/>
10. Документация для Python // Python documentation: <https://www.python.org/doc/>